PRO NETWORK
COUNTERFEIT GOODS & WIRE FRAUD

ON JULY 8, 2022 ONUR "ROY" AKSOY, WAS INDICTED by a federal Grand Jury in the District of New Jersey for one count of conspiracy to traffic in counterfeit goods and to commit mail and wire fraud; three counts of mail fraud; four counts of wire fraud; and three counts of trafficking in counterfeit goods in running a large-scale operation to traffic in fraudulent and counterfeit Cisco networking equipment. Additionally, seizure warrants were served on various financial institutions to recover criminal proceeds from AKSOY. The criminal indictment was the result of a Homeland Security Investigations (HSI) initiated criminal investigation that began in 2016 into PRO NETWORK (PN), a Cisco electronics broker located in Doral, Florida.

This investigation was part of Operation Chain Reaction (OCR), an HSI-led task force that proactively targets counterfeit goods entering the U.S government supply chain. By leveraging public-private partnerships, innovative data analytics, and the combined expertise of 17 federal agencies, OCR ensures the practical execution of supply chain risk management principles. U.S. Customs and Border Protection (CBP), Naval Criminal Investigative Service (NCIS), Defense Criminal Investigative Service (DCIS), General Services Administration Office of the Inspector General (GSA-OIG) all made notable contributions to the investigation.

Pro Network was identified as the highest volume importer of suspected counterfeit Cisco products. The main operator of Pro Network, Onur "Ron" AKSOY, wired at least $55 million to suppliers in Hong Kong and China for the purchase of the counterfeit Cisco products. The MSRP of the counterfeit products purchased by Pro Network since 2014 would have topped one billion USD had they had been genuine.

The Pro Network routers imported from China and Hong Kong were typically older, lower-model products, some of which had been sold or discarded, which Chinese counterfeiters then modified to appear to be genuine versions of new, enhanced, and more expensive Cisco devices. The Chinese counterfeiters would often add pirated Cisco software and unauthorized, low-quality, or unreliable components – including components to circumvent technological measures added by Cisco to the software to check for software license compliance and to authenticate the hardware. Many of these devices were sold to sensitive end users including the U.S. Navy, U.S. State Department, the Federal Bureau of Investigation (FBI), Boeing and other government aerospace contractors, and dozens of hospitals, urgent care facilities, and outpatient medical clinics.

Counterfeit electronics pose a significant health and safety threat, potentially having catastrophic outcomes. These outcomes include the potential to delay DOD missions, affect the reliability of weapon systems, imperil the safety of the warfighter, and endanger the integrity of sensitive data and secure networks.